IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCHES OF	
APPLE IPHONE 16 PRO MAX BEARING IMEI: 359222384700040, SERIAL NUMBER D3QMN6PGVL AND FBI BAR CODE NUMBER E8455460	Magistrate No. 25-476
8 GB USB DIGITAL STORAGE DEVICE BEARING FBI BAR CODE NUMBER E8455461	Magistrate No. 25-477
"SHERRETI" USB DIGITAL STORAGE DEVICE BEARING FBI BAR CODE NUMBER E8455462	Magistrate No. 25-478
SAMSUNG SOLID STATE DRIVE (SSD)-DISK DIGITAL STORAGE DEVICE BEARING SERIAL NUMBER S5GXNF0W629071J AND FBI BAR CODE NUMBER E8455463	Magistrate No. 25-479
HP LAPTOP COMPUTER BEARING SERIAL NUMBER CND9166DB8 AND FBI BAR CODE NUMBER E8455464	Magistrate No. 25-480
DESKTOP COMPUTER BEARING SERIAL NUMBER P000007519030913 AND FBI BAR CODE NUMBER E8455465	Magistrate No. 25-481
APPLE IPHONE 14 PRO MAX BEARING FBI BAR CODE NUMBER E8455466	Magistrate No. 25-482
CURRENTLY LOCATED AT 3311 EAST CARSON STREET, PITTSBURGH, PA 15203.	

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Micah Mayotte, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of a number of digital devices—which are currently in law enforcement possession — and the extraction of electronically stored information from that property described in Attachment B.

2. I am employed as a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since April 2022. I am currently assigned to the Pittsburgh Division of the FBI, on a squad which investigates computer and high-technology crimes, including computer intrusions, denial of service attacks and other types of malicious computer activity. I have been assigned to this squad since August 2022. I have received training and experience in computer crime investigations.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched consists of the following digital devices, ("SUBJECT DEVICES"):

a. Apple iPhone 16 Pro Max bearing IMEI: 359222384700040, serial number D3QMN6PGVL and FBI bar code number E8455460;

b. 8 GB USB digital storage device bearing FBI bar code number E8455461;

c. "Sherreti" USB digital storage device bearing FBI bar code number E8455462;

d. Samsung Solid State Drive (SSD)-Disk digital storage device bearing serial number S5GXNF0W629071J and FBI bar code number E8455463;

e. HP Laptop computer bearing serial number CND9166DB8 and FBI bar code number E8455464;

f. Desktop computer bearing serial number P000007519030913 and FBI bar code number E8455465; and

g. Apple iPhone 14 Pro Max bearing FBI bar code number E8455466.

5. The applied-for warrants would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On or about November 6, 2024, Ardit Kutleshi and Jetmir Kutleshi ("Defendants"), both citizens of Kosovo, were indicted by a federal grand jury sitting in the Western District of Pennsylvania at Criminal Case No. 24-248, based on the Defendants' administration and operation of the Rydox illicit marketplace ("Rydox"), which was hosted at rydox.cc, and the Defendants' receipt and use of criminal proceeds from Rydox. The six-count Indictment charges the Defendants with one count of conspiracy to commit money laundering in violation of Title 18, United States Code, Section 1956(h); one count of unauthorized solicitation of an access device in violation of Title 18, United States Code, Sections 1029(a)(6) and 2; one count of conspiracy to transfer, possession, or use a means of identification, in violation of Title 18, United States Code, Section 1028(f); two counts of unlawful transfer, possession, or use of a means of identification, in violation of Title 18, United States Code, Sections 1028(a)(7) and 2; and one count of aggravated identity theft, in violation of Title 18, United States Code, Section 1028A(a)(1) and 2 ("SUBJECT OFFENSES").

7. The FBI has been investigating Rydox since in or around November 2022 and the investigation revealed that the Defendants administered, operated, controlled, and maintained Rydox, which offered and sold illicit products and services to further online criminal conduct. These illicit products sold on Rydox included victims' personally identifiable information ("PII") such as names, addresses, dates of birth, and social security numbers, as well as stolen login credentials for e-mail accounts, passwords, e-commerce accounts, credit and debit card accounts, and online dating accounts. Rydox also sold cybercrime tools such as scam pages, spamming tools and spamming tutorials.

8. Based on an open-source review of the Rydox marketplace, the primary users of this online marketplace appear to be cybercriminals buying and selling stolen PII, stolen access devices and cybercrime tools. Further, the investigation revealed that the Defendants transferred criminal proceeds derived from Rydox's operation that exceeded the equivalent of greater than $10,000 and used criminal proceeds from Rydox to promote and operate Rydox.

9. In or around February 2016, Ardit Kutleshi created an account with the hosting services company, Qhoster, to host the domain "rydox.ru." The Qhoster account that hosted the domain rydox.ru was registered with the name Ardit Kutleshi and email flatearthbrotherhood@gmail.com. The Google account with email flatearthbrotherhood@gmail.com was registered with the phone number +38349140991 and recovery email ardit.kutleshi@yahoo.com. The Yahoo account with email ardit.kutleshi@yahoo.com was registered with the name "Rydox Cc," other identity "ardit.kutleshi," and the same recovery phone number (+38349140991).

10. In or around August 2017, Qhoster suspended Rydox's server account due to "dark market activities."

11. Soon thereafter, the Defendants created an account with a different web hosting company, Shinjiru, based in Malaysia, and transitioned Rydox to Shinjiru's servers. The subscriber information from web-hosting service provider Shinjiru showed that Ardit Kutleshi used his true name and the email address "flatearthbrotherhood@gmail.com," to register the account with Shinjiru.

12. Further, in or around March 2017, Jetmir Kutleshi created an account on a file sharing site (Mega.nz) to assist with the storage and transfer of the illicit products and services sold on Rydox. The Mega.nz account was registered with the email freshtools8@gmail.com. The Google account associated with email freshtools8@gmail.com was registered in the name "Ardit K," with recovery email logingelectronic@gmail.com and same recovery phone number (+38349140991) to register the other email accounts described above.

13. Analysis of the content of this email account, provided by Google in response to a search warrant, revealed that Ardit Kutleshi and Jetmir Kutleshi used freshtools8@gmail.com to register the Mega.nz and other accounts used to operate Rydox. A review of a search warrant return containing Facebook messenger communications between Ardit Kutleshi and Jetmir Kutleshi also revealed that the Defendants shared the password for the freshtools8@gmail.com account.

14. Rydox required its users to register on the site before being able to see what was for sale on the site or to sell any products on the site. Once a Rydox account was created and registered, a Rydox user could browse the Rydox marketplace for illicit services and products.

15. Upon clicking the "Reseller" link on Rydox, the site directed the user to the "Reseller" page, with information and procedures for becoming a reseller on Rydox. A "reseller" was a registered user of Rydox that was authorized to conduct sales on the site. Rydox resellers were required to pay a one-time fee in cryptocurrency which was sent to a cryptocurrency address associated with Rydox. The cost to become a reseller on Rydox fluctuated between $200 and $500 since Rydox's creation in 2016.

16. In or around April 2024, the "Reseller" information on the Rydox site stated that resellers would receive sixty percent (60%) of any proceeds from a sale and that Rydox would keep the remaining forty percent (40%) of sale proceeds. Resellers could choose their own price for the product they listed on Rydox. Rydox paid resellers their share of the sale proceeds every two weeks in cryptocurrency.

17. To make a purchase on Rydox, buyers were required to register with the site and then send cryptocurrency to an address provided by Rydox to establish credit with Rydox. The purchaser could then draw upon this credit to make purchases of illicit products on Rydox. Regardless of whether a Rydox user was sending cryptocurrency to Rydox to become a reseller or purchaser on the Rydox site, the funds sent to Rydox were placed in a cryptocurrency wallet controlled exclusively by Rydox and disassociated from user's account.

18. At least 1430 Bitcoin (BTC) wallet addresses were used by Rydox to accept payments from Rydox users and to send payments to Rydox resellers.

19. A review of the forensic image of the Rydox server that was obtained in 2023 from Shinjiru Technology ("Shinjiru"), the web hosting provider, and the cryptocurrency public ledger, revealed that the equivalent of approximately $232,284 USD in virtual currency had been

sent to deposit addresses controlled by Rydox between in or around September 2020 and in or around February 2023. During this same timeframe, Rydox received at least 3050 incoming virtual currency payments from registered Rydox users. The review of the Rydox server image also revealed that since at least 2016, Rydox completed at least 7600 transactions involving stolen PII, stolen access devices, means of identification, or cybercrime tools and services.

20. On or about September 19, 2022, Ardit Kutleshi, registered an account with the cryptocurrency payment processing provider CoinPayments with the account name "RydoxTeam" and User ID 3411423. The email "arbenkeci18@gmail.com" was also used to open this CoinPayments account. In addition, Ardit Kutleshi provided his genuine, Kosovo Driver's License (DL31049652) and his true date of birth (August 29, 1998) to comply with CoinPayments' Know Your Customer (KYC) requirements to open an account. The email arbenkeci18@gmail.com was attributed to the Defendants through cross referencing recovery e-mails and phone numbers connected to the Defendants.

21. When establishing the "RydoxTeam" CoinPayments account, an Instant Payment Notification ("IPN") function for URL https://rydox.cc /refill-crypto/ok was linked to the account so that the email account arbenkeci18@gmail.com (discussed above) received a notification each time a transaction was processed through the aforementioned URL. A review of a search warrant return for this same email account, arbenkeci18@gmail.com, and the deposit addresses associated with Rydox, corroborated that the "RydoxTeam" account at CoinPayments was used to facilitate payments to the Rydox marketplace.

22. The Defendants were arrested by Kosovo Police in Kosovo on or about December 12, 2024, based on a Provisional Arrest Request from the Federal Bureau of Investigation and

are expected to be extradited to the Western District of Pennsylvania to face prosecution related to the SUBJECT OFFENSES.

23. During the arrest of the Defendants, the Kosovo Police collected several pieces of evidence, including the SUBJECT DEVICES. The digital devices listed in paragraphs 4.a-f were collected from Ardit Kutleshi and the device listed in paragraph 4.g was collected from Jetmir Kutleshi pursuant to a Mutual Legal Assistance Treaty (MLAT) request to Kosovo.

24. After seizing the SUBJECT DEVICES incident to the Defendants' arrest, the Kosovo Police transferred them to the FBI also pursuant to the MLAT request. Therefore, while the FBI might already have all necessary authority to examine the SUBJECT DEVICES, I seek this warrant out of an abundance of caution to be certain that an examination of the SUBJECT DEVICES will comply with the Fourth Amendment and any other applicable laws.

25. The SUBJECT DEVICES are currently in storage at 3311 East Carson Street, Pittsburgh, PA 15203. In my training and experience, I know that the SUBJECT DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICES first came into the possession of the FBI.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication

through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online, I know that the SUBJECT DEVICES listed in paragraphs 4.a and 4.g have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I also know that electronic devices, such as the SUBJECT DEVICES can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on a digital device. This information can sometimes be recovered with forensics tools.

29. There is also probable cause to believe that things that were once stored on the devices listed in paragraphs 4.b-f may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of their use, who used them, and when. There

is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on a digital storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on a storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can also record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to create and operate a cybercrime marketplace, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

32. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

33. I submit that this affidavit supports probable cause for search warrants authorizing the examination of the SUBJECT DEVICES described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

s/Micah Mayotte
Micah Mayotte
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 24th day of March 2025.

_____
HONORABLE PATRICIA L. DODGE
United States Magistrate Judge

ATTACHMENT A

34. The property to be searched consists of the following digital devices, (hereinafter "SUBJECT DEVICES"):

a. Apple iPhone 16 Pro Max bearing IMEI: 359222384700040, serial number D3QMN6PGVL and FBI bar code number E8455460.

b. 8 GB USB digital storage device bearing FBI bar code number E8455461

c. "Sherreti" USB digital storage device bearing FBI bar code number E8455462

d. Samsung Solid State Drive (SSD)-Disk digital storage device bearing serial number S5GXNF0W629071J and FBI bar code number E8455463

e. HP Laptop computer bearing serial number CND9166DB8 and FBI bar code number E8455464

f. Desktop computer bearing serial number P000007519030913 and FBI bar code number E8455465

g. Apple iPhone 14 Pro Max bearing FBI bar code number E8455466

The SUBJECT DEVICES are currently in the FBI evidence locker located at 3311 East Carson Street, Pittsburgh, PA 15203.

This warrant authorizes the forensic examination of the SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the SUBJECT DEVICES described in Attachment A that relate to violations of the SUBJECT OFFENSES and involve Ardit Kutleshi and Jetmir Kutleshi since between on or about February 1, 2016, and on or about December 12, 2024, including:

a. Records and information relating to unlawful access to other individuals online accounts;

b. Records and information relating to possession or sale of access devices, personal information, or account credentials;

c. Records and information relating to the sale or use of tools related to spamming, scam pages or other online fraud;

d. Records and information relating to the sale of intellectual property, including television shows and movies, protected by U.S. copyright laws;

e. Records and information relating to the facilitation of money laundering, money laundering services, including unauthorized cryptocurrency exchanges;

f. Records and information relating to the acquisition or sale of sexually explicit content created or shared (i.e. leaked) without the user's consent;

g. Records and information relating to the administration, marketing, and support of Rydox.cc and Rydox.ru;

h. Records and information relating to communications with the owners and administrators of Rydox.cc and Rydox.ru;

i. The identities of all other individuals involved in administering Rydox.cc and Rydox.ru;

j. Communications with individuals involved in administering Rydox.cc and Rydox.ru;

k. Evidence of who used, owned, or controlled the device being searched, such as such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

l. Evidence of software that would allow others to control the device being searched, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

m. Evidence of the lack of such malicious software;

n. Evidence indicating how and when the device being searched was accessed or used to determine the chronological context of the access, use, and events relating to the SUBJECT OFFENSES and to the user of the device being searched;

o. Evidence of the attachment to the device being searched of other storage devices or similar containers for electronic evidence;

p. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device being searched;

q. Evidence of the times the device being searched was used;

r. Passwords, encryption keys, and other access devices that may be necessary to access the device being searched;

s. Documentation and manuals that may be necessary to access the device being searched or to conduct a forensic examination of the device being searched;

t. Records of or information about Internet Protocol addresses used by the device being searched;

u. Records of or information about the device being searched's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

v. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.